

772
United States Senate
WASHINGTON, DC 20510
September 21, 2016

COMMITTEES:
BANKING
DEMOCRATIC POLICY & COMMUNICATIONS
FINANCE
JUDICIARY
RULES

The Honorable Jeh Johnson
Secretary
Department of Homeland Security
245 Murray Lane, S.W.
Washington, D.C. 20528

The Honorable Thomas Wheeler
Chairman
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Dear Secretary Johnson and Chairman Wheeler:

I write to express my deep concern surrounding a recent report that exposed serious vulnerabilities within our 911 emergency system. Given the findings of this research, I urge you to convene a working group and conduct a top-to-bottom investigation into our nation's 911 system. I hope that you will be able to make recommendations and, where possible, implement new regulations to plug the holes in the system.

As you know, a report completed by researchers from the Ben Gurion University revealed that a bot attack on mobile phones could block emergency services in an entire state, for days. By infecting mobile phones, and using those phones to surreptitiously overwhelm 911 call center lines, attackers would be able to fully disable 911 services. For the state of North Carolina, in which this research was conducted, it would take a mere 6,000 bots for attackers to disrupt the state. Given that a state as large as North Carolina could be so easily manipulated, I am extremely concerned that this threat could severely harm New York and the rest of our nation's 911 services if duplicated in mobile phones across America.

The Department of Homeland Security (DHS), in tandem with the Federal Communications Commission (FCC), is tasked with ensuring the safety of our communication networks. Currently, 911 centers and networks lack the technical ability to block calls made by infected phones or handle the resulting level of abnormal call volumes. With nearly 80% of 911 calls coming in from mobile phones, it is critical that our nation's emergency infrastructure is equipped to defend against all malicious cyber-attacks.

At a time when our country is facing heightened risk for attack, both physical and digital, it is imperative that our 911 emergency systems remain secure and available to continue providing services around the clock. I hope you will swiftly address this issue and identify and implement solutions that will strengthen our 911 cybersecurity needs. Should you need any assistance or have legislative recommendations, please feel free to contact my staff.

Thank you and I look forward to working with you on this issue in the future.

Sincerely,



Charles E. Schumer
United States Senator





FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

October 21, 2016

The Honorable Charles E. Schumer
United States Senate
322 Hart Senate Office Building
Washington, D.C. 20510

Dear Senator Schumer:

Thank you for your letter regarding vulnerabilities in the Nation's 911 system. I share your concern about the need to secure the physical and logical infrastructure of the nation's 911 call centers, also known as Public Safety Answering Points (PSAPs). The Ben Gurion University's research paper that you cited in your letter presents a compelling case study of the theoretical risks that PSAPs must be prepared to protect against, detect, and respond to in order to ensure that members of the public have uninterrupted access to 911.

The Nation's PSAPs are at a crossroads as the Next Generation 911 transition challenges them to depart from a reliance on legacy, analog systems to state of the art digital, IP-based systems. The End of Life period for legacy technologies can be the most dangerous for ensuring cybersecurity of information technology and communications infrastructure. NG911 can, however, enable PSAPs to manage incoming 911 calls effectively and to institute robust call routing policies to better handle and deflect disruptive denial of service attacks.

In fact, earlier this year, the FCC's Task Force on Optimal PSAP Architecture (Task Force), an expert advisory panel, adopted a comprehensive set of recommendations and guidance that could help accelerate the nation's transition to NG911, including methods to protect PSAPs effectively and efficiently against the real and expanding threat of cyber-attack as they transition from the circuit-switched world. Later this year, the Task Force will deliver a detailed set of recommendations regarding establishing Emergency Communications Cybersecurity Centers to conduct inspection and filtering of PSAP call traffic. I anticipate that the Task Force's recommendations will serve as the foundation for further concerted industry top-to-bottom investigation of the how to protect PSAPs from cyber and denial of service attacks. We have and will continue to work closely with industry and our agency partners to identify, mitigate and where possible reduce cybersecurity risk.

In multiple testimonies before Congress, I have suggested that the FCC is close to the limit of what it can do to facilitate NG911 and called on Congress to take action to create national enablers to accelerate the transition to NG911, lower its cost to PSAPs, and institute critical cybersecurity protections.

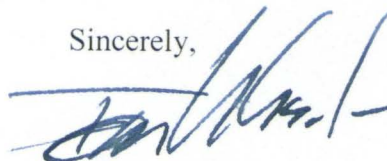
We need coordinated action and leadership at both the state and national level to guarantee that our 911 emergency systems remain secure and available to provide services

Page 2—The Honorable Charles E. Schumer

around the clock. Congress has the unique ability to make the transition to NG911 a national priority and to provide the means to achieve it.

I appreciate your interest in this matter. Please let me know if I can be of any further assistance.

Sincerely,

A handwritten signature in blue ink, appearing to read "Tom Wheeler", with a stylized flourish at the end.

Tom Wheeler

